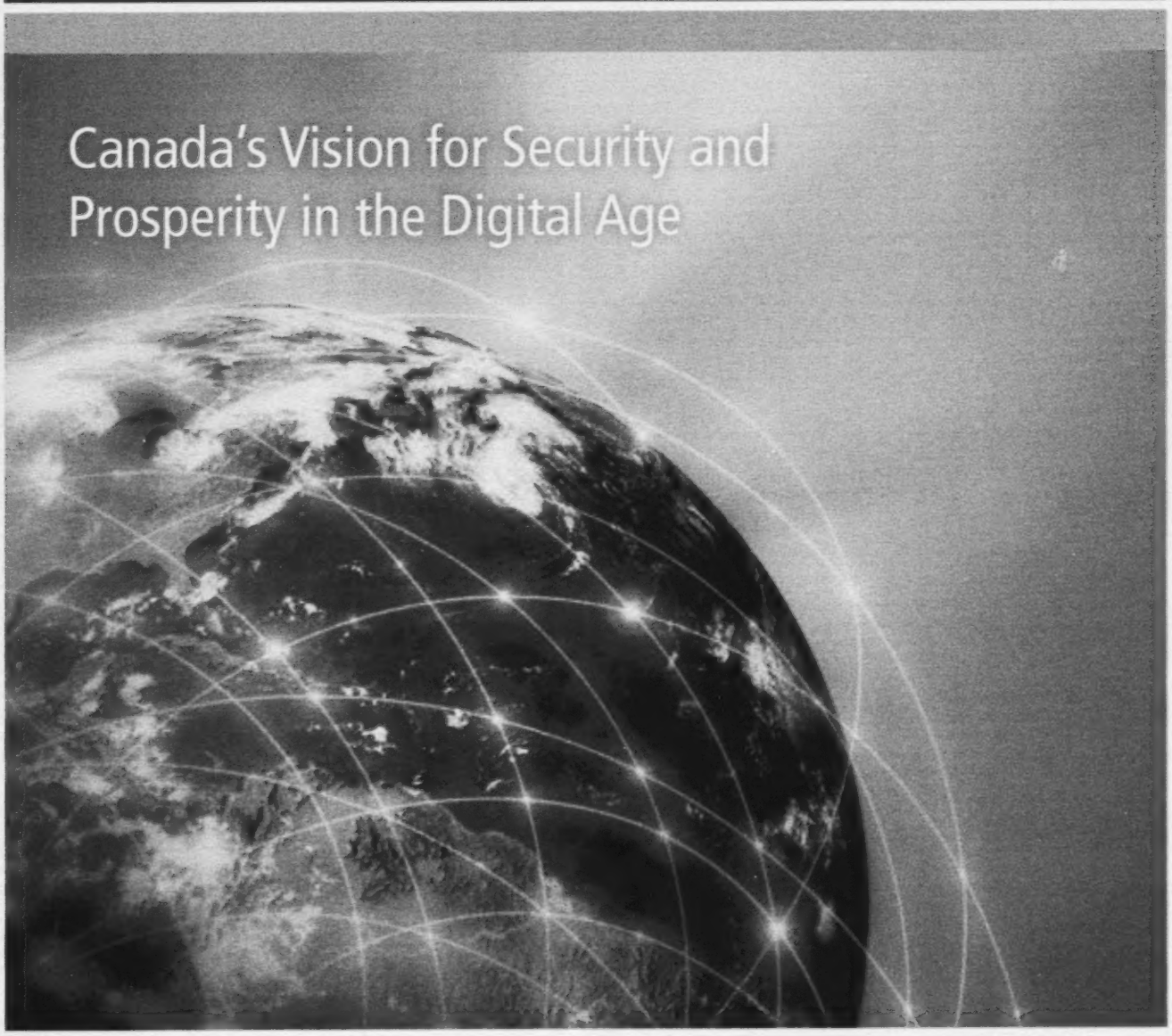
Public Safety Canada | Sécurité publique Canada

Canada

National Cyber Security Strategy

Canada's Vision for Security and Prosperity in the Digital Age



© Her Majesty the Queen in Right of Canada, 2018

Cat. No.: PS4-239/2018E
ISBN: 978-0-660-26553-7

Table of Contents

Executive Summary 1

- Canada's Place in a Digital World
- The Importance of Cyber Security
- The Vision of the National Cyber Security Strategy: Security and prosperity in the digital age
- Scope of the Strategy
- Implementing the Strategy

Introduction 7

- Building on Canada's Accomplishments in a Dynamic Cyber Landscape

Security and Resilience 12

- Strategic Context: The Evolution of the Cyber Threat
- Cybercrime and Advanced Cyber Threats
- The Growing Impact
- Public Consultation on Cyber Security
- Secure and Resilient Canadian Systems

Cyber Innovation 19

- Strategic Context: Expanding Frontiers of Cyber Security
- New Horizons of Technology and Business Development
- Building on the Benefits of Digital Technology
- Advancing 21st Century Skills and Knowledge
- Public Consultation on Cyber Security
- An Innovative and Adaptive Cyber Ecosystem

Leadership and Collaboration 26

- Strategic Context: Collaborating to Realize the Benefits of Digital Life
- Raising Baseline Cyber Security in Canada
- Federal Cyber Security Leadership in a Dynamic Environment
- Public Consultation on Cyber Security
- Effective Leadership, Governance, and Collaboration

Workbook Glossary 33

Foreword

THE HONOURABLE RALPH GOODALE

Minister of Public Safety and Emergency Preparedness Canada

Virtually everything Canadians do is touched by technology in some way – on a per capita basis, we spend the most time online of any country in the world, at 43.5 hours per Canadian per month. We are heavily interconnected and networked, a fact that enhances our quality of life, but also creates vulnerabilities. From commercial supply chains to the critical infrastructure that underpins our economy and our society, the risks in the cyber world have multiplied, accelerated, and grown increasingly malicious.

Major corporations, industries and our international allies and partners are engaged in the global cyber challenge. But many others are not — representing a significant risk, but also a missed opportunity in this rapidly growing global industry. While it is important to be keenly aware of cyber threats, Canada's cyber security policy cannot be driven by fear and defensiveness.

With this in mind, the renewal of the existing Cyber Security Strategy has been undertaken with an emphasis on the enormous potential of Canada's increased leadership in this field. In partnership with the Ministers of Defence, Innovation, Infrastructure, Public Services and the Treasury Board, we consulted directly with Canadians and key stakeholders about how the new strategy could best serve their security needs, while allowing them to benefit from the opportunities that the digital economy offers. Informed by over 2,000 submissions to our public consultation, the Strategy directly addresses the gaps and areas for improvement in Canada's current cyber security climate.

The Strategy's core goals are reflected in Budget 2018's substantial investments in cyber security – totaling more than $500 million dollars over five years. As the largest single investment in cyber security ever made by the Canadian government, Budget 2018 demonstrates our commitment to safety and security in the digital age.

Among the new measures introduced:

- Funding for the new Canadian Centre for Cyber Security to support leadership and collaboration between different levels of government and international partners, while providing a clear and trusted resource for Canadian citizens and businesses.
- The creation of the National Cybercrime Coordination Unit to expand the RCMP's capacity to investigate cybercrime, establishing a coordination hub for both domestic and international partners.
- Funding to foster innovation and economic growth, and the development of Canadian cyber talent.

The Strategy is the roadmap for Canada's path forward on cyber security, and is designed to meet the objectives and priorities of Canadians. We are proud to be leading the way.

Executive Summary

Canada's Place in a Digital World

Our world has been transformed by digital innovation.

Digital technologies are now an integral part of our daily lives, with new developments emerging every day. From running our businesses, accessing government services, to interacting with our friends and families, these technologies connect Canadians from coast to coast to coast while linking us into a dynamic global network.

This is just the beginning. There is endless potential for new and revolutionary ideas. We will continue to see digital innovation pushed to new heights — to the benefit of our communities, our societies, and our planet.

Executive Summary

The Importance of Cyber Security

As we embrace digital technologies for their tremendous benefits, we can open ourselves up to threats.

Criminals and other malicious cyber threat actors — many of which operate outside our borders — take advantage of security gaps, low cyber security awareness, and technological developments in an effort to compromise cyber systems. They steal personal and financial information, intellectual property, and trade secrets. They disrupt and sometimes destroy the infrastructure that we rely on for essential services and our way of life.

In 2010, the Government of Canada launched a national effort to defend against these threats with Canada's first Cyber Security Strategy. The progress made and accomplishments achieved under the 2010 Strategy are the basis for future action.

Our new approach reflects the extent to which digital technologies have become essential to our way of life. With a new Cyber Security Strategy, we can proceed with confidence in our digital age. In this reality, cyber security is the companion to innovation and the protector of prosperity.

The Vision of the National Cyber Security Strategy: Security and prosperity in the digital age

Strong cyber security is an essential element of Canadian innovation and prosperity. Individuals, governments, and businesses all want to have confidence in the cyber systems that underpin their daily lives. The Government of Canada envisions a future in which all Canadians play an active role in shaping and sustaining our nation's cyber resilience.

Executive Summary

To realize our vision, the Government of Canada and its partners will work together across three themes:

Security and Resilience

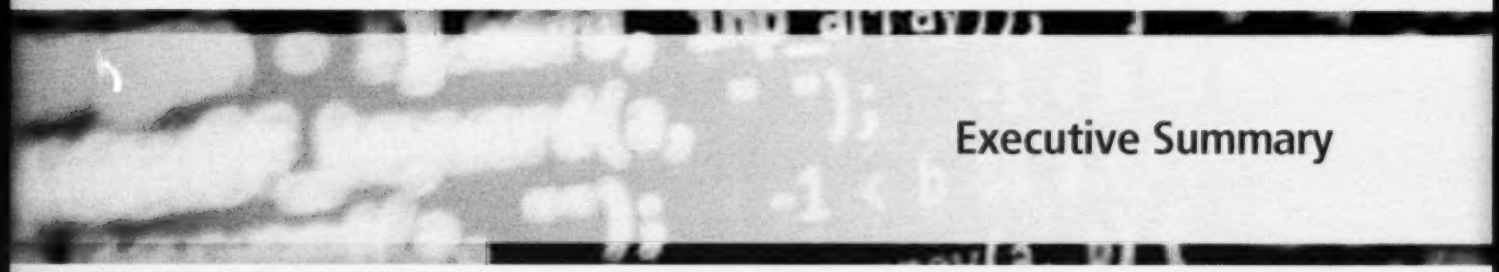
Through collaborative action with partners and enhanced cyber security capabilities, we will better protect Canadians from cybercrime, respond to evolving threats, and defend critical government and private sector systems.

Cyber Innovation

By supporting advanced research, fostering digital innovation, and developing cyber skills and knowledge, the federal government will position Canada as a global leader in cyber security.

Leadership and Collaboration

The federal government, in close collaboration with provinces, territories, and the private sector, will take a leadership role to advance cyber security in Canada and will, in coordination with allies, work to shape the international cyber security environment in Canada's favour.



Executive Summary

In a dynamic cyber security environment, the Government of Canada's approach will be rooted in a sustained commitment to:

- Protect the safety and security of Canadians and our critical infrastructure
- Promote and protect rights and freedoms online
- Encourage cyber security for business, economic growth, and prosperity
- Collaborate and support coordination across jurisdictions and sectors to strengthen Canada's cyber resilience
- Proactively adapt to changes in the cyber security landscape and the emergence of new technology

Scope of the Strategy

The scope of this Strategy starts with the work that the Government of Canada is already undertaking. This includes ongoing and future efforts to protect Government of Canada systems, to extend our network of partnerships to help protect critical infrastructure, and to help Canadians to be safe online. In a more diverse and dynamic global cyber security landscape, however, Canada's new approach will be more extensive and inclusive. This document outlines the key elements of the global cyber security environment and articulates some of the ways that the Government of Canada will respond to an array of new challenges and opportunities in cyberspace.

Implementing the Strategy

Recognizing that the pace of change we see today will only accelerate, this Strategy is designed as the mainstay of the Government's continuous efforts to enhance cyber security in Canada. The Government's actions will evolve alongside the ground-breaking technological developments and resulting paradigm shifts that have become common in our connected world.

Cyber security action plans will supplement this Strategy. These will detail the specific initiatives that the federal government will undertake over time, with clear performance metrics and a commitment to report on results achieved. They will also outline the Government's plan for working with internal and external partners to achieve its vision.

The implementation of this Strategy will align with other cyber-related Government of Canada initiatives. These include: the Minister of Democratic Institutions' mandate to defend the electoral process from cyber threats; cyber foreign policy in Canada's international agenda; the Canadian military's use of cyber; and the Innovation and Skills Plan.

Canada's Cyber Security Strategy 2010

The Government of Canada's first Cyber Security Strategy allocated $431.5 million over ten years, with three pillars of action and wide-ranging accomplishments:

I. Securing Government systems

The Government of Canada increased its capacity to prevent, detect, respond to, and recover from cyber attacks. The number of data breaches has steadily declined since 2010 — despite an increase in the number and sophistication of state-sponsored and non-state cyber activities against Government networks.

II. Partnering to secure vital cyber systems outside the federal government

Partnerships were forged with owners and operators of Canada's critical infrastructure, the private sector, and provincial and territorial governments. The Canadian Cyber Incident Response Centre (CCIRC) expanded its operations, with over 1300 organizations receiving regular alerts and communications.

III. Helping Canadians to be secure online

Through the Get Cyber Safe campaign, the Government of Canada supported cyber security awareness with outreach, activities, and development of targeted resources. Efforts made under the 2010 Strategy also improved the capacity of the RCMP and law enforcement agencies to combat cybercrime, including initial investments in cybercrime intelligence, investigations, and training.

Introduction

Building on Canada's Accomplishments in a Dynamic Cyber Landscape

What is Cyber Security?

Cyber security is the protection of digital information and the infrastructure on which it resides.

Cyber security was once the domain of technical experts, but now, in our digital world, we all have a role to play in our individual and collective cyber security.

From the Margins to the Mainstream

The degree to which digital technology is now integrated into our daily lives would have been unimaginable just a few years ago. From social media, smartphone applications, online shopping, networked devices, the cloud, and beyond, we rely on digital technologies for more than personal enjoyment — they are integral to the systems that underpin our economy and our way of life. These interdependent systems include the

communications networks that connect across the country and around the world, energy to heat our homes and power our industry, and air, train, and road travel we use every day.

We tend to take this connectivity for granted, without pausing to reflect on its implications. Cyber security cannot be taken for granted. As the benefits and opportunities of technologies continue to grow, it is increasingly crucial to secure these technologies.

Taking Stock of a Changing Landscape

In 2016, the Government of Canada took the first step toward developing a new Cyber Security Strategy. The Cyber Review was launched to understand the cyber security implications of being a connected nation, and to position the Government of Canada to establish a new approach that reflects the challenges and opportunities we face.

The Cyber Review sought to take stock of the evolving threats in cyberspace, to understand and explore the ways that cyber security is becoming a driver of economic prosperity, and to determine the appropriate federal role in this digital age. The Cyber Review included in-depth engagement within the federal government cyber security community, an evaluation of our performance under the 2010 Strategy, as well as Canada's first public consultation on cyber security. The Government of Canada obtained insights and advice from experts, key stakeholders, and engaged citizens.

CYBER SECURITY SNAPSHOT: THE BENEFITS OF BACKING UP

Jacqueline is a small business owner who sells crafts through an online store. One day, Jacqueline receives an email from a customer who is complaining about a broken piece. The customer attaches a picture of the product, but when Jacqueline opens the attachment she finds that she is locked out of her computer. A message appears indicating that her computer will only be unlocked if she pays a ransom of $1,000 to the perpetrator. Fortunately, Jacqueline regularly backs up her computer. She wipes her hard drive, eliminating the malware that was delivered through the email attachment and restores the backup, which allows her to access all her documents.

Introduction

Our Response

This new Cyber Security Strategy reflects the perspectives from the Cyber Review. It also recognizes that while cyber threats are growing in sophistication and magnitude, there is enormous potential for Canadian digital innovation and expertise in cyber security. It is designed to be adaptable and to account for a continuously changing cyber landscape.

Our National Cyber Security Strategy establishes three goals in response to evolving threats, emerging opportunities, and the need for collaborative action:

- Secure and Resilient Canadian Systems
- An Innovative and Adaptive Cyber Ecosystem
- Effective Leadership and Collaboration

The federal government will lead the effort to achieve these goals in an era when cyber security is not just a necessity, but a competitive advantage for Canada.

CYBER SECURITY SNAPSHOT: PASSWORD SMARTS

Christine loves the convenience of the cloud. She created one central account online that manages everything from her computer, her smartphone, her fitness tracker, and even her home security system. Through the cloud, her email and social media accounts are linked, her photos and videos are uploaded automatically, and any updates to her calendar appear across all her devices. Christine always uses the same password so that it's easy for her to remember. When she hears about a data breach affecting her email account, she realizes that someone could use her email password to access her cloud account. Concerned about protecting her privacy and her information, Christine creates a new, strong password, which she varies slightly for other online services.

About the Cyber Security Review

The input received through the Cyber Review was comprehensive, sophisticated, and insightful. Responses came from the federal government cyber community, cyber security experts, business leaders, government officials, law enforcement, academics, and engaged citizens.

The Cyber Review revealed three main trends:

There is support for law enforcement's efforts to address cybercrime while protecting privacy in cyberspace

- There is recognition that cyber security serves to protect personal information — and by extension, privacy. Canadians support efforts to safeguard their privacy online.
- Canadians acknowledge that law enforcement faces challenges addressing cybercrime, and are concerned by the rising threat of cybercrime for individuals, private and public sector organizations, and governments.

There is a wide ranging need for improved cyber security knowledge and skills

- Better cyber security knowledge and skills are needed. This extends from our children to our elderly and from our small and medium business owners to our law enforcement agencies and corporate executives.
- A shortage of cyber security talent makes it difficult for organizations — including the federal government — to attract and retain the people they need to improve their cyber security or to disrupt cyber threats.

About the Cyber Security Review

There are calls for strong federal leadership on cyber security:

- External partners want a reliable focal point of federal government leadership on cyber security.
- Partners want consistent messaging, advice, guidance from the Government of Canada.
- Organizations have asked for cyber security standards or legislation in Canada to clarify requirements and expectations to improve their cyber security.
- Stakeholders want to see federal leadership in cyber security to foster national collaboration, drive investment, facilitate information sharing and safeguard rights and freedoms.

Security and Resilience

Strategic Context: The Evolution of the Cyber Threat

The threats we face in cyberspace are complex and rapidly evolving. Governments, businesses, organizations, and Canadians are vulnerable. With more of our economy and essential services moving online every year, the stakes could not be higher.

Cybercrime and Advanced Cyber Threats

Perpetrators of malicious cyber activity are extremely diverse, with varying aims and a wide array of techniques. Malicious cyber actors include individual hackers and insider threats, criminal networks, nation states, terrorist organizations, and state-sponsored actors. Sophisticated cyber attacks are often technically challenging to understand, with significant expertise required to do so.

Security and Resilience

Any organization or individual can be a victim of malicious cyber activity. Victims may be individually targeted or part of a campaign affecting millions of internet users. As Canadians put more information online, they become increasingly attractive targets for malicious cyber actors. Canadian law enforcement agencies' ability to protect Canadians from these actors, who may be anywhere in the world, is a growing challenge.

Malicious cyber activity is often conducted for monetary gain. For example, phishing emails that appear to come from financial institutions can deceive people into providing their banking information. Ransomware can be deployed to encrypt files on a device or system, with a hacker demanding payment to restore access. Data breaches can result in personal and financial information (such as social insurance numbers, credit card information) being stolen from organizations' online databases and subsequently sold in criminal marketplaces for activities like fraud, identity theft, or extortion.

Malicious cyber actors can also be motivated by a specific cause — sometimes called "hacktivists" — such as exposing wrongdoing, protesting, or provoking embarrassment. They can also be enthusiasts, attempting to demonstrate their skill at hacking and to gain notoriety.

On a larger scale, nation states and state-sponsored actors have the capability to steal our intellectual property or confidential business strategies to give their own economies a competitive advantage.

Some nation states are also developing advanced cyber tools with hostile aims. There are risks to Canada's national security and public safety if

the threat is to the computer systems that underpin government systems, critical infrastructure, and democratic institutions. Terrorist organizations are also interested in acquiring advanced cyber tools to conduct attacks.

The Growing Impact

As malicious cyber tools become increasingly accessible and as rates of cybercrime continue to rise, there is a real threat to Canada's economic well-being. Furthermore, as more of Canada's critical infrastructure can be controlled remotely and essential services are managed online, cyber incidents have the potential to compromise national security and public safety.

From a financial perspective, victims of cyber compromise face immediate costs to recover and restore their systems. They also face long-term costs to replace or upgrade cyber systems, as well as untold reputational costs. While start-ups are particularly vulnerable, the loss of intellectual property has contributed to financial ruin for businesses of all sizes.

Cyber incidents can also be profoundly destabilizing. They can erode trust in e-commerce and government institutions and can lead people to question their continued use of digital technologies if they feel that their safety or privacy is at risk.

The **internet-of-things** (IoT) refers to objects and devices that are connected to the internet to communicate with one another and provide

CYBER SECURITY SNAPSHOT:
EMAIL SCAMS

It's tax season and Mohsen recently filed his taxes online. A few days later, he receives an email from someone claiming to be a tax official, informing him that there is information missing from his file. The official makes an urgent request for additional personal information to complete his file, including his address and social insurance number. The email notes that failure to provide this information could lead to steep penalties and even jail time. Mohsen feels suspicious about the email, and so before providing the information, he checks the Canada Revenue Agency (CRA) website. He reads that the CRA would never send emails asking individuals to divulge personal or financial information. He follows the CRA's advice by ignoring the email.

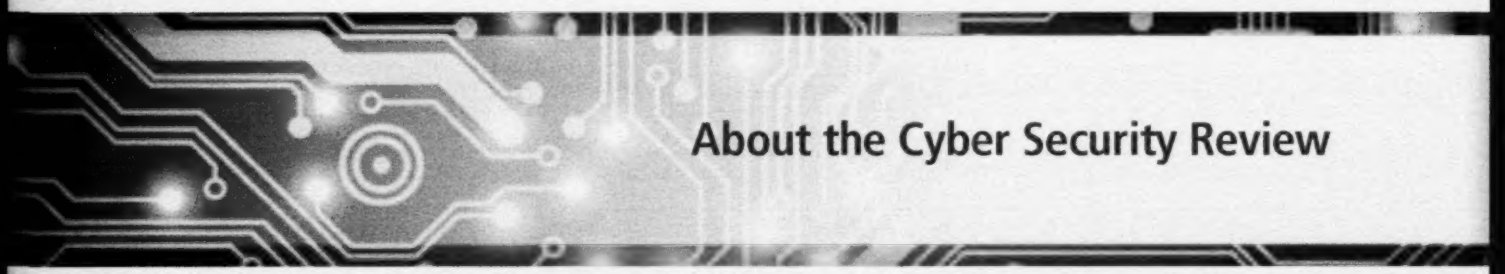
more efficient and customized services. The IoT is growing rapidly, with over 25 billion connected devices expected by 2020.

Connecting devices to the internet opens the door to new cyber security risks. Cyber security gaps can be exploited to disrupt services through distributed denial of service (DDoS) campaigns or to gain entry to wider systems or private data. In October 2016, millions of unsecured devices were used to overwhelm the servers of Dyn, an internet infrastructure company, which then took popular websites and online services offline internationally.

As digital innovation is pushed further and as new technologies are developed, the nature of cyber threats will constantly change. For instance, internet-connected technologies are increasingly popular, from thermostats and healthcare devices like pacemakers to cars and the systems that run our critical infrastructure and services. Without adequate cyber security, connected devices are vulnerable to being hacked on an unprecedented scale. Similarly, many Canadians rely on encryption to secure their online communications and data. The arrival of quantum computing will undercut the security of traditional encryption, requiring that Canadians have quantum-resistant solutions at their disposal. A forward-looking and flexible cyber security posture will be necessary to keep pace with these changes.

CYBER SECURITY SNAPSHOT: RESILIENCE THROUGH INFORMATION SHARING

Beom-Jun works in the IT Department for a large financial institution. He has noticed that there have been a lot of attempts to hack into the system. While they have been unsuccessful, he decides to send the technical information to the Canadian Cyber Incident Response Centre (CCIRC) for their analysis. He knows that CCIRC relies on critical infrastructure organizations, like his bank, to report cyber incidents so that they can notify other sectors and international partners of trends and threats. He appreciates that by working together, they are increasing the cyber security of the organizations that Canadians rely on.



About the Cyber Security Review

Public Consultation on Cyber Security

What We Heard

"The #1 cyber challenge for Canada is that there are an increasing number of incidents that are causing harm to the economy and society, ranging from breaches, crimes, disruption of essential services, and destruction of corporate and country assets"

"Privacy and security are not a zero-sum game and we can have both. There is no security without privacy. And liberty requires both security and privacy"

"Canadian law enforcement should centralize their cybercrime resources... A single window centre will make it easier for businesses to know who to call when their systems have been compromised, and will help law enforcement investigate and respond to cybercrime across jurisdictions"

Secure and Resilient Canadian Systems

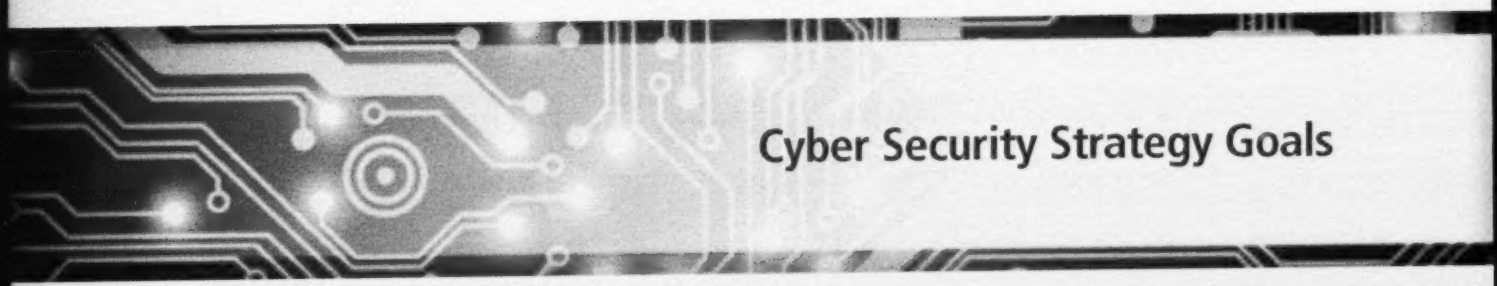
Through collaborative action with partners and enhanced cyber security capabilities, we will better protect Canadians from cybercrime, respond to evolving threats, and defend critical government and private sector systems.

The Government of Canada will maintain and improve cyber security across all federal departments and agencies to protect the privacy of Canadians' information held by the federal government and the confidentiality, integrity, and availability of critical services for Canadians.

The Government of Canada will enhance law enforcement capacity to respond to cybercrime. It will support coordination across law enforcement agencies and with federal, provincial, territorial, and international partners. The Government will enhance cybercrime investigative capacity and make it easier for Canadians to report cybercrime.

Small and medium organizations often lack the knowledge and resources to implement cyber security regimes, even if doing so would offer a competitive advantage. The Government of Canada will help support these organizations — making cyber security more accessible.

In response to cyber threats of increasing sophistication, the Government of Canada will consider how its advanced cyber capabilities could be applied to defend critical networks in Canada and deter foreign cyber threat actors.



Cyber Security Strategy Goals

Some cyber systems — such as electricity grids, communications networks, or financial institutions — are so important that any disruption could have serious consequences for public safety and national security. The federal government will work with provinces, territories, and the private sector to help define requirements to protect this digital infrastructure.

Cyber Innovation

Strategic Context: Expanding Frontiers of Cyber Security

Digital innovation has become the engine of economic growth in the 21st century. Cyber security is not only essential for protecting the sources of Canada's digital innovation — it has become a source of innovation in its own right.

New Horizons of Technology and Business Development

Cyber security is increasingly driving innovation and economic activity in Canada. It already contributes $1.7 billion to Canada's GDP and consists of over 11,000 well-paying jobs.[1] With the global cyber security industry forecasted to grow by 66% by 2021, thousands of additional jobs could

CYBER SECURITY SNAPSHOT:
SKILLS FOR THE DIGITAL AGE

Marc is looking for possible summer camps for his daughters. He wants to find something that allows them to try something different while developing new skills. In his search, he comes across a summer program designed to help children develop basic coding skills, which would give them the tools they need to build websites and develop their own programs. With Marc's encouragement they register for the camp, opening the door to a new hobby and an exciting skillset.

1 International Data Corporation (IDC) Canada , "2016 Canadian ICT Predictions and Forecast: Digital Transformation and Disruption," December 2015; Information and Communications Technology Council (ICTC), "Critical Infrastructure in a Hyperconnected Economy," August 2016.

be created for Canadians in the years ahead.[2] Governments, academia, and members of the private sector can work together to create new opportunities, drive investment, and foster leading-edge research and development.

Canada is already a leader in cyber security research and development. Breakthroughs in cyber security research are not only beneficial for Canadian cyber security firms, but for the economy as a whole. Government has a role to play to support advanced research and to help innovative companies scale up to bring cyber security technologies and services to the global marketplace.

Building on the Benefits of Digital Technology

Canada's participation in digital life has generated immense prosperity and benefits, and has opened a new gateway to the world. Governments, businesses and other organizations play a central role in protecting these benefits by establishing strong security for their online platforms, products, and services.

Cyber security is only as strong as its weakest link. Small and medium enterprises — and indeed many organizations in Canada — face similar challenges securing their systems and networks as their much larger counterparts, but must do so with less expertise and fewer resources. Governments can help correct this asymmetry by providing advice and guidance and enhancing access to cyber security information and tools.

CYBER SECURITY SNAPSHOT:
STREAMLINING SERVICE DELIVERY

Stuart was relieved when he found out that he could access his Canada Pension Plan (CPP) account online without having to remember another password. All he has to do is go to the CPP log-in page, click on the logo for his bank, and enter his information. He uses the same username and password as he does for his online banking, since his bank is a sign-in partner for the Government of Canada's online services. He really likes the convenience, and since he trusts his bank's security measures, he knows his information is protected. As his son David keeps telling him, his banking information will be safer as long as he uses a secure Wi-Fi — like his password-protected network at home. Apparently, hackers can intercept traffic over unsecured Wi-Fi, like in a coffee shop or airport.

2 Research and Markets, "Cyber Security Market – Global Forecast to 2021," August 2016.

This helps Canadian organizations in both public and private sectors to successfully adopt digital technologies.

Individual knowledge goes a long way in cyber security, from digital literacy all the way to coding and threat mitigation skills. Initiatives in Canadian communities, schools, and post-secondary institutions help to equip Canadians with skills for the digital age. The Government of Canada is playing its part through long-term investments to help Canadians of all backgrounds to get the education and work experience they need to participate in an increasingly digital economy.

Quantum science and technology allows information to be processed and secured much more rapidly and more securely. Quantum devices could have revolutionary benefits across a range of fields, such as helping to understand how diseases develop or optimizing medical treatments. While quantum can secure information and push technology to new limits, its use may also threaten many forms of encryption used today to protect systems and applications in Canada and around the world.

Recognizing the opportunities and challenges of quantum computing, Canadian efforts have established a strong base of expertise and leadership in quantum computing, like that seen at the Institute of Quantum Computing at the University of Waterloo.

Advancing 21st Century Skills and Knowledge

The demand for qualified cyber security professionals is surging. A global shortage of qualified professionals represents an immediate and growing opportunity for Canada's highly educated workforce. We can encourage more students to move into science, technology, engineering, and mathematics (STEM) fields. We can encourage graduates from both STEM programs and other disciplines (such as psychology, sociology, or management) to specialize in the skills needed for cyber security jobs. Attracting this multidisciplinary talent, both domestically and from abroad, is essential for Canadian governments and businesses. It also helps to ensure that Canadian companies are able to safely grow and innovate as they expand their use of digital technology.

As the cyber security environment continues to evolve, there is a constant need for reliable and up-to-date information. Canadian statistics and research in the area of cyber security will provide a more accurate view of the cyber issues our nation faces in a global context. This information can be used by academics, researchers, and policy makers to understand trends, manage risk, inform future investments, and adjust course when appropriate.

About the Cyber Security Review

Public Consultation on Cyber Security

What We Heard

"We must work to ensure that start-ups and innovation born in Canada stay in Canada"

"The federal government can play a unique role in ensuring businesses see Canada as a location where they can thrive in a cyber safe environment"

"Few appreciate the strategic relevance of cyber security intelligence. You can't manage what you don't measure"

An Innovative and Adaptive Cyber Ecosystem

By supporting advanced research, fostering digital innovation, and developing cyber skills and knowledge, the federal government will position Canada as a global leader in cyber security.

The Government of Canada will work with partners to drive investment and foster cyber research and development. The Government will focus on emerging areas of Canadian excellence, such as quantum computing and blockchain technologies. The federal government is already making progress in this regard, with Budget 2017 announcing the creation of a Pan-Canadian Artificial Intelligence Strategy for research and talent.

Together, we will explore initiatives to ensure that Canadian companies can bring their products to a global market. The Government will explore initiatives to drive domestic demand for cyber security technologies and services.

The Government of Canada will explore new ideas for making businesses and Canadians of all ages and backgrounds more cyber secure. The federal government has already committed investments to improve digital skills, such as coding education for kids.

Working together across governments, academia, and the private sector is necessary to address the cyber skills gap. Taking action now will allow us to build the labour force of the future, one that will help to support Canadian cyber security and that will contribute to Canada's future prosperity.

Cyber Security Strategy Goals

The quality of information at our disposal shapes our ability to understand cyber trends. The federal government will support Canadian research and statistics efforts to improve our collective understanding of cyber threats and opportunities.

Leadership and Collaboration

Strategic Context: Collaborating to Realize the Benefits of Digital Life

Advances in technology benefit our communities and our societies. They contribute to our quality of life today, and will be instrumental in meeting the challenges of tomorrow. We all have a responsibility to secure these technologies. Through our National Cyber Security Strategy, the Government of Canada will advance the ways in which we work together to do so.

Raising Baseline Cyber Security in Canada

The vast majority of Canada's digital systems are owned by individuals and organizations outside of the federal government. From individuals that use few technologies to tech-savvy businesses that are firmly rooted in the online world, many do not realize that they could be the target of cyber threats. As a result, they do not have measures in place to protect

themselves and recover from cyber incidents. Even those that recognize the importance of securing their information may find it hard to identify affordable and effective measures to protect themselves.

The Government of Canada is taking on a leadership role in cyber security to help organizations and Canadians recognize the value of cyber security and to support efforts to raise the baseline of cyber security in Canada. It will complement these domestic efforts by working with international partners and allies, seeking to reduce the threat to Canada from cybercriminals and also from state actors and their proxies that may seek to harm us.

Moreover, the federal government is aiming for national cyber security excellence. Reaching this target will involve enhancing and growing cyber security capabilities in government and industry. It will entail supporting Canada's leading edge research and development, as well as the range of organizations and businesses that do not have strong cyber security measures in place. Private sector leaders will have a central role to play, as a collaborative effort is needed to ensure that all Canadians are as equipped as possible to prevent and respond to cyber threats.

Blockchain technology allows for the creation of online ledgers or records. Often associated with virtual currencies, there are many possible applications of blockchain. It could be used to provide public services like issuing passports, creating records of contracts or legal documents, and processing payments for services rendered. The technology improves efficiency by reducing processing time for activities and reduces the risk of fraud and compromise, as no one party can modify, delete or append any records.

Leadership and Collaboration

The Government of Canada recognizes the potential of blockchain for secure service delivery and for wider economic and societal benefits. Ensuring the smart application of blockchain technologies in Canada will require a collaborative approach and a collective effort.

Federal Cyber Security Leadership in a Dynamic Environment

The Government of Canada is in a unique position to play a leadership role in cyber security. This stems from extensive relationships with private and public sectors, a history of working with provinces, territories, and international officials on a range of cyber security issues, and advanced cyber security expertise and capabilities.

Federal leadership in cyber security was established through the 2010 Strategy and the nation-wide initiatives it introduced. In today's cyber security environment, however, the federal government must deepen collaboration with partners to strengthen Canada's cyber security. Concerted and integrated action by all parties is needed to build cyber resilience in Canada.

Establishing a clear focal point for cyber security within the federal government is one of the ways that the Government will demonstrate leadership while also enhancing its capacity to collaborate with partners. The Government will ensure that partners receive unified advice and guidance on cyber security and that they know where to go for assistance.

Leadership and Collaboration

Smart cities use digital technologies to enhance quality of life by making services more efficient, cost-effective, and responsive for urban residents. For example, "smart" traffic lights will measure and adapt timing to improve traffic flows and connected sewer systems will detect leaks and monitor real-time water flow.

To accelerate the development of smart cities in Canada, the federal government announced the Smart Cities Challenge initiative in Budget 2017.

The federal government will make smart investments in cyber security, while also advocating for its partners in the private sector and in other jurisdictions to do the same. Private sector organizations in Canada have world-class cyber security capabilities that can be leveraged to benefit all sectors of the Canadian economy. There are also great ideas and strong leadership in our schools and our post-secondary institutions that will be instrumental in shaping the future of cyber security in Canada.

The Government will work to bridge Canada-wide efforts to develop cyber skills, advance new solutions, and strengthen cyber security. We will be an example to the world of what can be achieved through a cohesive and coherent National Cyber Security Strategy.

CYBER SECURITY SNAPSHOT: COLLABORATING TO SOLVE CYBER SECURITY PROBLEMS

Augustine received an invitation to participate in the Canadian Cyber Incident Response Centre's (CCIRC) annual Geek Week. He attended last year and enjoyed working with cyber professionals and academics from Canada and other countries to solve cyber security problems. Augustine found that the skills and professional connections he gained during Geek Week benefitted him when he returned to work. At last year's event, his team experimented with CCIRC's prototype tools to perform automated analysis of mobile-based malware and ransomware, and also examined how encryption on such devices can be exploited by attackers. He likes that the work they did can have a real-world benefit and that after the event the team was able to take the tool they worked on back to their own organizations to develop further.

Public Consultation on Cyber Security

What We Heard

"The Government of Canada can provide much needed leadership by creating, adopting and modeling best practices for cyber security, and making efforts to transfer this knowledge to the private sector"

"[There is a] need for more centralized governance and strategic planning ... for modern legislation and regulations, and leadership in identifying, prioritizing, endorsing and disseminating the latest international standards of cyber security technology"

"Collectively, we need to create an effective framework for cyber security governance, spanning principles, roles, and responsibilities within the government and across the public and private sectors"

Effective Leadership, Governance, and Collaboration

The federal government, in close collaboration with provinces, territories, and the private sector, will take a leadership role to advance cyber security in Canada and will, in coordination with allies, work to shape the international cyber security environment in Canada's favour.

Responding to calls for decisive federal leadership, the Government of Canada will streamline the way it works and collaborates with external partners and stakeholders by establishing a clear focal point for authoritative advice, guidance, and cyber incident response. This approach will improve information sharing and make it easier for the private sector to obtain the support it needs.

The Government of Canada will reinvigorate public awareness and engagement efforts and establish new forums for collaboration. The federal government will work in consultation with a cross-section of Canadian stakeholders to ensure that we collectively enhance cyber security in Canada.

The federal government will lead, in partnership with provinces, territories, and the private sector, the development of a national plan to prevent, mitigate and respond to cyber incidents, one that ensures efficient coordination and effective action.

Cyber Security Strategy Goals

The Government of Canada will work with its international partners to advance Canadian interests. This includes advocating for an open, free, and secure internet and enhancing our international cooperation to combat cybercrime.

Workbook Glossary

App/Application

An application, especially as downloaded by a user to a mobile device (for example, fitness tracking app).

Artificial Intelligence

The subfield of computer science concerned with developing intelligent computer programs that can solve problems, learn from experience, understand language, interpret visual scenes, and, in general, behave in a way that would be considered intelligent if observed in a human.

Blockchain

A blockchain is a write-only database dispersed over a network of interconnected computers that uses cryptography (the computerized encoding and decoding of information) to create a tamperproof public record of transactions. Blockchain technology is transparent, secure and decentralised, meaning no central actor can alter the public record.

Cloud Computing

The ability to access all required software, data and resources via a computer network instead of the traditional model where these are stored locally on a user's computer.

Critical Infrastructure

Processes, systems, facilities, technologies, networks, assets and services essential to the health, safety, security or economic well-being of Canadians and the effective functioning of government. Critical infrastructure can be stand-alone or interconnected and interdependent within and across provinces, territories and national borders. Disruptions of critical infrastructure could result in catastrophic loss of life, adverse economic effects and significant harm to public confidence.

Cyber Attack

An attack that involves the unauthorized use, manipulation, interruption or destruction of, or access to, via electronic means, electronic information or the electronic devices or computer systems and networks used to process, transmit or store that information.

Cyber Incident

Any unauthorized attempt, whether successful or not, to gain access to, modify, destroy, delete or render unavailable any computer network or system resource.

Cyber Security

The protection of digital information, as well as the integrity of the infrastructure housing and transmitting digital information. More specifically, cyber security includes the body of technologies, processes, practices and response and mitigation measures designed to protect networks, computers, programs and data from attack, damage or unauthorized access so as to ensure confidentiality, integrity and availability.

Cyber Threat

A threat actor, using the internet, who takes advantage of a known vulnerability in a product for the purposes of exploiting a network and the information the network carries.

Cybercrime

A crime committed with the aid of, or directly involving, a data processing system or computer network. The computer or its data may be the target of the crime or the computer may be the tool with which the crime is committed.

Cyberspace

The electronic world created by interconnected networks of information technology and the information on those networks. It is a global commons where more than 3 billion people are linked together to exchange ideas, services, and friendship.

Data Breach

The unauthorized disclosure of information that compromises the security, confidentiality, or integrity of personally identifiable information.

Distributed Denial of Service (DDoS)

A type of denial of service attack in which an attacker uses a malicious code installed on various computers to attack a single target.

E-Commerce

The buying and selling of information, products and services via the internet.

Encryption

Cryptology is discipline that embodies principles, means, and methods for the transformation of data in order to hide its information content, prevent its undetected modification and/or prevent its unauthorized use. The conversion of the information into this new protected form is referred to as encryption. The conversion of information back to its original form is decryption.

Hacker

Someone who uses computers and the Internet to access computers and servers without permission.

Insider Threat

A malicious threat to an organization that comes from people within the organization, such as employees, former employees, contractors or business associates, who have inside information concerning the organization's security practices, data and computer systems.

Intellectual Property (IP)

According to the World Intellectual Property Organization, intellectual property (IP) is a creation of the mind. IP includes inventions, literary and artistic works, designs and symbols, and names and images used in business.

Internet-of-things

The interconnection via the internet of computing devices embedded in everyday objects, enabling them to send and receive data.

Malicious Software/Malware

Malicious software designed to infiltrate or damage a computer system, without the owner's consent. Common forms of malware include computer viruses, worms, Trojans, spyware, and adware.

Quantum Computing

A quantum computer can process a vast number of calculations simultaneously. Whereas a classical computer works with ones and zeros, a quantum computer will have the advantage of using ones, zeros and "superpositions" of ones and zeros. Certain difficult tasks that have long been thought impossible for classical computers will be achieved quickly and efficiently by a quantum computer.

Ransomware

Software that denies you access to your files until you pay a ransom.

Smart Cities

Smart cities use digital technologies to enhance quality of life by making services more efficient, cost-effective, and responsive for urban residents.

Spear Phishing, Phishing

The use of fraudulent emails to persuade people within an organization to reveal their usernames or passwords. Unlike phishing, which involves mass mailing, spear phishing is small-scale and well targeted.